Online Safety Policy Issues – A Global Report

Emma Morris

Good morning,

Firstly let me say that it is a real pleasure to be here. As Jillian said I manage international policy for FOSI. My work covers a broad spectrum of issues including online safety, privacy, security, data protection as well as certain criminal laws as they relate to online behaviors. In terms of geographies up until now we have focused on the United States, Europe and particularly the UK but now increasingly our work will encompass Australia and New Zealand.

The last few years have been exceedingly busy as Internet safety and privacy have moved up governments' agendas around the world. There has been a broad range of responses with autocratic regimes choosing extreme blocking of content, though not always with purely safety motivations, whilst other countries have opted for an industry led self-regulatory approach, with a more hands-off government. The majority of countries have fallen somewhere in the middle of the spectrum.

Today I hope to shed some light upon current initiatives, policies and laws from the UK, Europe and America that are shaping the global Internet landscape in which we all operate.

We'll start with the UK since that has occupied the majority of my working day, and a little beyond that, for the past week. The debate over child abuse material aside for now, the UK has long been a leader in the online safety space. In 2008, following the report from Professor Tanya Byron, the government established the United Kingdom Council on Child Internet Safety or UKCCIS. This brought together over 200 organizations to work to ensure that children experienced all of the great opportunities of the online world, whilst minimizing the risks. Initially the output included voluntary codes of

practice as well as better information and education on issues surrounding Internet safety for parents and children.

UKCCIS survived the change in governments and in 2011 a report from Reg Bailey entitled “Letting Children Be Children - Report of an Independent Review of the Commercialisation and Sexualisation of Childhood” updated the remit of the Council and filtering and parental controls became the focus. The concept of ‘active choice’ was developed providing customers with an unavoidable choice during installation as to whether or not to block adult content. The definition of ‘adult content’ has been largely assumed to cover pornography, violence, gambling and sites that promote self-harm or suicide. It remains the case that users must decide whether to switch-on filters. The alternative proposed would have meant that filters would be default on and users would have to contact their ISP to opt-out this was known as ‘Active Choice Plus’.

Certain child safety advocates and government ministers wanted more and were not satisfied with the introduction of ‘Active Choice’ alone. Consequently by the end of 2013 each of the 5 largest ISPs in the UK will be providing parental controls that can be set for the whole home with one device, as well as the creation of family friendly, or filtered, Wi-Fi in public places.

Whilst the UK can be applauded for their commitment to the online safety issues, the move towards default filtering for adult material was concerning. Research carried out by FOSI showed that the majority of parents were excising controls, technological or otherwise, over their children’s access to the Internet. Not to mention the argument that filtering systems have a tendency to block legitimate websites and limitations on legal, though potentially harmful, content can be hard to justify in a democratic country.

That brings me back to the debate over child abuse material that has raged in the UK for the past couple of weeks. Ultimately the ISPs and Google provided two million pounds to improve the discovery and take down of child abuse content, as well as committing to a

zero tolerance statement and deliverables that were already being pursued through UKCCIS.

A concerning trend that we saw, which needs to be guarded against, was the conflation of illegal and legal content. Importantly blocking does not solve the problem at all; this is an issue that requires an international rather than purely domestic response.

Moving now to Europe.

The European Union has a long history of activity in this space. The Safer Internet Program has been running for many years, providing funding to the reporting hotlines and the Safer Internet Centres throughout the continent. However in late 2011 the Commissioner for the Digital Agenda, and Vice-President of the Commission itself, Neelie Kroes declared that more needed to be done. She focused on the services being offered by the big Internet companies operating in Europe and demanded that they do more to protect the privacy and safety of European children using their platforms.

The Commissioner wrote directly to the CEOs of these companies outlining the key strategic areas on which she hoped to make advancements, these included;

- simple tools for users to report harmful content and contact;
- age-appropriate privacy settings;
- wider use of content classification;
- wider availability and use of parental controls; and
- the effective take down of child abuse material.

And so the CEO Coalition for a Better Internet for Kids was born.

Lengthy meetings followed throughout 2012, a failure in performance from any of the working groups carried with it the possibility of legislation. In February 2013, on Safer Internet Day to be specific, each of the working groups reported back to the Commission on their progress. Output varied between working groups but included;

- the creation of apps for the reporting of harmful content;
- an interactive database containing current practices regarding privacy settings for minors;
- a self-certification scheme for apps based on an online assessment;
- the roll out of parental controls by all Coalition members; and
- a renewed pledge to improve takedown times of reported child abuse material.

Additionally each of the industry members was required to make their own specific commitments. Responses ranged and depended upon the applicability of the objectives of each working group to companies. Some Coalition members limited themselves to restating the past year's achievements and committing themselves to the deliverables laid out by each working group. Others went further. Notable commitments included the creation of the post of Chief Online Safety Officer and the appointment of a Child Safety Officer in each country as well as in-store training sessions for parents when purchasing mobile phones for their children.

Thus far 2013 has been a year for delivery against these assurances. At a meeting held this month with the Commissioner, she declared herself satisfied with the progress that was being made and saw no immediate need for legislation.

Not to be outdone by the Commission, industry responded to the work of the CEO Coalition by forming their own self-regulatory group in early 2012, confusingly it is also called a 'coalition' but this time it's the 'ICT Coalition for a Safer Internet for Children and Young People.' The group aims to develop innovative ways of enhancing online safety and encouraging responsible use of the Internet. The focus of this group has tended to err more on the side of awareness raising, rather than the specific deliverables that have been seen in the other coalition.

In our opinion at FOSI the most important initiative was launched in May 2012 as a joint effort by Commissioners Kroes, Reding and Malmstrom. The strategy built upon much of what is contained within the CEO Coalition, aiming to equip children with the skills that

they will need for the future, but it went further. It challenges industry, with the support of the Commission and Member States to improve upon the interactive, creative and educational content online for children. At FOSI we advocate that materials need to be created for children in order that they are able to access age appropriate content and so that they can ultimately build the necessary knowledge and resilience to participate fully in the digital world.

Finally, conversations around privacy in Europe are not complete without briefly looking at the reforms to the data protection laws. In 2012 proposals were made to update the 1995 Directive, unsurprisingly they mostly focus on those who engage in the processing of personal information. However, the Regulation goes further than the previous law. The most controversial provision is probably article 17 which introduces the right to be forgotten which would allow users the right to request that their personal data be deleted and, moreover, that where data is shared with a third party, the first party service would be required to inform the third party of that deletion request. Far from minimizing the data that is stored, which is the ultimate aim of the Regulation, article 17 would in massively increase data retention in addition to placing huge burdens on companies.

The overall objective of the reforms is to create a digital single market with uniform rules and increased consent requirements further cementing the commitment to individual privacy in Europe. However, to date there have been over 3,000 amendments filed by the European Parliament, numerous delays and intense lobbying against the Regulation, especially by American companies. The next few months will tell whether the new law will pass by the end of this Commission next year and if so, in what form and with what compromises.

Moving to America.

The United States has been warily watching Europe for the past couple of years, and the concern was heightened by the data protection proposals. Although a majority of the

Internet companies are based in the US, the European reforms that allow for fines up to 2% of global turnover certainly had industry executives and US politicians worried.

The heightened consent requirements for the processing of children's data would bring the EU in line with the US position under the Children's Online Privacy Protection Act but that Rule itself has undergone changes and revisions in the past year.

At the end of last year the Federal Trade Commission released its much awaited revisions to the Rule that supplements COPPA. For those who aren't familiar with the Rule it is the one that prevents companies from collecting and processing the personal information of children under the age of 13 without their parents' consent. It's why many of the services that you use, even here in Australia, require you to be 13. It's a practice that industry has decided to implement around the world in the absence of other laws. Contrary to many peoples' beliefs it has nothing to do with the safety or the appropriateness of the site.

The new text has divided opinion amongst industry and privacy advocates. Real concern was expressed regarding the potential impact on the availability of online content for children under the age of 13 as well as the cost and feasibility of compliance for small businesses and app developers. Whereas other changes have been welcomed, the promotion of just-in-time notifications makes sense and will assist parents in making informed decisions about what their kids are doing online.

The new Rule comes into force in the US in 7 days and we will have to wait and see what the impact will be.

In Washington, DC, on Capitol Hill, lawmakers have considered a wide range of proposals from Do Not Track laws to those that focus on data breach notification and preventing online piracy. Most relevant to children's online safety was the Do Not Track Kids Act from 2011. In addition to extending COPPA protections to those over 13 it incorporated the concept of an 'eraser button.' This would allow parents, not teens themselves, to request that information about their child be deleted. Serious First

Amendment concerns were raised and we are told that the bill will be rewritten before it is introduced again in this session.

Individual states in the US have also been incredibly active. Whether it be proposing their own versions of COPPA or updating criminal statutes to include cyberbullying as a criminal offense or imposing different punishments for the sending of sexually graphic images by teenagers.

Action is not confined to the legislative branch in America, the US Administration issued its privacy framework in February 2012 calling for baseline privacy protections for all and do not track as standard. The National Telecommunications and Information Administration, effectively the President's advisors on technology and Internet issues, has been working with stakeholders to develop short form privacy notifications for mobile apps. In a process that has now taken a year we are told that we are incredibly close to reaching consensus.

More and more my role and has become that of an interpreter. On the one hand I am explaining the motivations behind European initiatives to baffled US lawmakers. Whilst at the same time underlining the US' commitment to fostering innovation, carefully weighed against protections, when speaking to confused representatives from Europe.

As the CEO Coalition shows the Europeans are looking to Silicon Valley for industry leadership, and the 'eraser button' concept and its similarities to the 'right to be forgotten' demonstrate that the US isn't blind to European action either. Both are keen to promote innovation and ensure that children are able to access the massive opportunities that the Internet provides. Governments around the world should remember that all children are going to need digital skills in the future in order to fully participate in all areas of their lives.

If there is one area that we at FOSI would encourage all Governments, with industry cooperation, to focus on, it is the creation of educational, creative and fun content for children of all ages.

As for this year, the current levels of legislative activity in Washington, DC, London and Brussels suggests that the final six months of 2013 may shape the landscape around children's online safety and privacy for many years to come.